unosecur

WHITEPAPER

Identity security for BFSI sector

Identity Security: The Unosecur Advantage

Table of contents

Executive summary

The Banking, Financial Services, and Insurance (BFSI) sector is facing rapidly evolving challenges – from emerging threats to compliance requirements. As a trusted par tner of several key players in the sector, Unosecur is deeply at tuned to these issues. The digital transformation of this industry has created remarkable oppor tunities but also brought about unprecedented risks, par ticularly in the realm of identity security. The shif t to cloud-based systems, the surge in both human and machine identities, and the rising capabilities of AI systems have created a complex security landscape that demands immediate and sophisticated solutions.

This white paper delves into the intricacies of identity threats within the BFSI sector, examining the vulnerabilities caused by over provisioned access, weak authentication protocols, and the explosive grow th of machine identities. As highlighted, over 93% of organizations experienced two or more identity-related breaches last year, underscoring the urgent need for robust identity access management (IAM) strategies. From mitigating insider threats to combating advanced tactics, such as deepfake impersonation enabled by generative AI, the risks are as diverse as they are severe. Unosecur has assessed these challenges and identified that traditional approaches to identity security no longer suf fice in multi- cloud environments. Financial institutions must adopt comprehensive IAM frameworks that integrate multi-factor authentication, privileged access management, and real-time threat detection. The case for proactive identity security measures is clear – every breach not only endangers sensitive data but also erodes customer trust and financial stability.

At Unosecur, we have pioneered solutions tailored to address the unique demands of the BFSI sector. Our suite of tools – including the IAM Analyzer, NHI Dashboard, and Identity Fabric enables organizations to secure their identity perimeters, ensure compliance, and swif tly adapt to emerging threats. By combining cut ting- edge technology with an in- depth understanding of BFSI dynamics, Unosecur empowers businesses to safeguard their digital assets and foster resilience in an increasingly volatile cyber landscape.

This white paper invites you to gain a deep understanding of the need for identity security in BFSI. At Unosecur, we are commit ted to being your trusted par tner in identity security, delivering not just solutions, but a strategic vision for a secure and sustainable future.

Introduction

Identity security in the BFSI sector: Growing risks & need for compliance

Businesses in the banking, financial ser vices, and insurance (BFSI) sector worldwide are scrambling to get their act together on cybersecurity regulations.
While BFSI businesses in the EU region are struggling to meet the DORA regulations deadline, the latest Financial Stability Report by the Reser ve Bank of India emphasises the importance of cybersecurity in bank-related payment systems and mandates access management controls as a foundational pillar for securing digital payment systems.

In India, over 70% of customer complaints reported in Q1 and Q2 of FY 2024-25 are related to electronic and mobile banking fraud. This comes hot on the heels of the warning issued by the Finance Ministry in November 2024 , directing public sector banks (PSBs) to align their cybersecurity practices with industry standards. Add to this the threat of vulnerabilities introduced by generative AI technologies, and the situation worsens drastically.

A white paper published by the Bank for International Settlements, titled Generative AI and Cybersecurity in Central Banking, highlights Gen AI- enabled vulnerabilities, such as social engineering, deepfake impersonation, and unauthorised data disclosure.

According to the report , these threats can lead to:

- Unauthorised access to internal banking networks
- Privacy breaches and sensitive data leaks
- Erosion of trust in financial institutions and potential risks to financial stability

The possibility of unauthorised access and identity-based at tacks in the BFSI sector has never been higher. Safeguarding operations with the urgent adaptation of identity access management (IAM) measures, such as multi-factor authentication (MFA), privileged access management (PAM), and role -based access control (RBAC), is crucial in addressing these risks.

Put simply, effective IAM systems can mitigate these risks by:

- Enforcing adaptive authentication to detect and block anomalous login at tempts.
- Securing employee and customer identities across all touch points.
- Protecting access to cloud infrastructure and ensuring business continuity in the face of identity-based at tacks.
- Reducing the risk of account takeovers and operational disruptions caused by credential theft or compromised identities.

However, to address these challenges effectively, we must first understand the basics of cloud identity threats.

Understanding cloud identity threats

What are cloud identity threats?

Cloud identity threats refer to risks associated with managing identities and access within cloud environments. As organizations transition to the cloud, user credentials and permissions become key targets for attackers.

These threats often exploit weak passwords, misconfigured access controls, or stolen credentials to gain unauthorized access to critical systems and data. In cloud environments, identities—both human and machine—serve as the new security perimeter, making cloud identity management essential.

The evolution of cloud identity threats:

In the early days of cloud computing, identity management was relatively simple, with fewer integrations and straightforward credential management. Security practices focused on static credentials, such as passwords, to manage access, and systems relied heavily on manual oversight to handle permissions. These setups mirrored traditional IT environments, prioritizing predefined roles and limited scalability.

As cloud environments have evolved, so have the threats. Today, dynamic cloud setups involve thousands of human and machine identities with granular permissions. Attackers exploit weak access controls, misconfigured APIs, and overprivileged accounts to infiltrate systems. The integration of third-party services and the rapid adoption of automation tools have further expanded the attack surface. Additionally, threats such as lateral movement, privilege escalation, and insider misuse require continuous monitoring and adaptive security measures.

Major identity threats: The MITRE ATT&CK framework

The MITRE ATT&CK framework is a comprehensive knowledge base of adversary tactics and techniques used in cyber attacks. Here are the phases of the framework that show how attackers progress in exploiting identity vulnerabilities to gain access, escalate privileges, and exfiltrate sensitive data from cloud environments.

1. **Compromised Credentials:**
   How it happens: Phishing, brute force, or stolen passwords.
   Impact: Attackers escalate privileges and move laterally in systems.

2. **Initial access via APIs:**
   How it happens: Weak access controls or unsecured APIs.
   Impact: Attackers gain higher privileges, modify security settings, and perform unauthorised actions.

3. **Exfiltration of sensitive data:**
   How it happens: APIs or compromised accounts are used to steal data.
   Impact: Theft of valuable, sensitive information.

4. **Persistence through cloud accounts:**
   How it happens: Exploiting or creating service accounts.
   Impact: Maintaining access to systems even after initial compromise.

5. **Access misconfigurations:**
   How it happens: Poorly defined permissions and overprivileged accounts.
   Impact: Orphaned accounts and exploitable access combinations.

AI agents and identity security

As artificial intelligence continues to evolve, so do its roles in the enterprise. AI agents—autonomous software entities powered by large language models—are quickly becoming embedded across business operations, from handling DevOps workflows to automating customer support. But while these agents deliver immense value, they also introduce a new class of identity-based risks that traditional security tools aren't equipped to handle. The core technologies enabling AI agents, Model Context Protocol (MCP) and the Token Vault, also fuel the prospects of serious identity security risks. Here's how.

Understanding AI agents, MCP, and Token Vault

AI Agents: The new autonomous workforce
AI agents are no longer simple chatbot interfaces. They can read emails, manage cloud infrastructure, pull analytics reports, and act on behalf of users, without a human in the loop. But with this autonomy comes a problem: how do you control and secure a digital entity that doesn't have a face, a name, or a password?

What Is MCP (Model Context Protocol)?
MCP is the emerging standard that allows AI agents to interact with external applications and systems securely and consistently. Developed initially by Anthropic, it provides a standardized way for AI agents to query systems, access resources, and execute commands: all with context-aware controls.

Think of MCP as the secure communication bridge. The AI agent uses it like a universal translator, converting its task request into a system-specific API call while ensuring security checks are baked into every interaction.

Key Features of MCP:

- Context-aware authentication using OAuth 2.1 tokens
- Standardized language for accessing diverse systems
- Dynamic permissioning based on AI task context and user role

What Is Token Vault?
Token Vault is the AI's secure key management system. Rather than embedding access credentials directly in AI agents, enterprises use Token Vaults to store, issue, and manage access tokens in real time.

Token Vault:
- Grants short-lived, scoped tokens only when the AI agent needs them
- Handles token refresh and revocation, reducing human intervention
- Abstracts credentials, so the AI agent never sees raw usernames, passwords, or API keys
- Works well with OAuth 2.0 flows and compliance-friendly access logs

Together, MCP and Token Vault allow AI agents to behave like enterprise users: querying systems, initiating actions, and integrating across tools, without compromising access security.

The top three AI identity security risks

Risk crops up when these capabilities are misused. For instance, stolen tokens can lead to accumulation of privileges, or extension of existing ones. As we know now, AI agents have access to sensitive systems, yet operate differently from human users or services. This creates identity vulnerabilities that security teams must proactively address.

Privilege accumulation
AI agents often start with narrow permissions, but as their roles expand, they quietly accumulate more access rights than necessary, particularly when there is no Token

Vault. This “AI privilege creep” leads to the creation of stale roles, over-provisioned tokens, and unnecessary exposure.
Why it matters: A compromised or misbehaving AI agent with excessive privileges can alter cloud configurations, read customer data, or escalate its own access, without being flagged.

Prompt Injection
AI agents interpret natural language prompts. Attackers can exploit this by feeding malicious instructions that bypass the AI’s built-in safety guardrails, causing it to take unintended actions.
Why it matters: A single misleading prompt can cause an AI agent to output confidential data or trigger a dangerous workflow, without breaching any technical perimeter.

Token Theft
Tokens stored or transmitted insecurely can be intercepted or leaked, allowing attackers to impersonate the AI agent. This threat is amplified when AI agents handle access tokens for multiple services.
Why it matters: A leaked token is equivalent to a stolen identity. It allows full access to the target system, bypassing both the AI and the user who authorized it.

Threat Landscape

The common attacks listed under the MITRE ATT&CK framework and the AI-related threats often exploit vulnerabilities such as weak access controls, misconfigured APIs, overprivileged accounts, and stolen credentials. The rise of enhanced AI agents and the growing complexity of multi-cloud environments make it difficult to secure these systems. Understanding the threat landscape and the common challenges helps us understand what we need in our security stack.

Threat Scale in a nutshell

80% Percentage of financial organizations concerned about vulnerabilities resulting from overprovisioning third-party identities.

Source: HelpNet Security, December 2024

77% Percentage of investment firms rank vulnerability to cyberattacks as a top factor impacting their transformation plans.

Source: Mayer Brown, December 2024

93% Percentage of organizations that experienced two or more identity-related breaches in 2023.

Source: Hindu Businessline, July 2024

88% Percentage of cybersecurity breaches globally caused by human errors.

Source: IBM's 2022 Cost of a Data Breach Report.

61% Percentage of breaches caused by compromised credentials.

Source: Verizon's 2022 Data Breach Investigations Report

Challenges in determining and securing the identity perimeter

Securing the identity perimeter involves managing and protecting digital identities across various platforms, devices, and networks. Key challenges include:

Complexity
With the proliferation of cloud services and mobile devices, managing a vast number of user identities becomes increasingly complex. Ensuring consistent access controls and monitoring across diverse systems is a significant hurdle.

Insider threats
Employees or contractors with legitimate access can intentionally or unintentionally compromise security, making it essential to monitor and manage internal risks effectively.

Regulatory compliance
Adhering to various data protection regulations requires stringent identity management practices, adding to the complexity of securing the identity perimeter.

Traditional cloud environments

In traditional cloud settings, organizations face specific identity security challenges.

Misconfigurations
Incorrectly configured identity systems can create vulnerabilities, allowing unauthorized access to sensitive data. Regular audits and proper configuration management are essential to mitigate this risk.

Blind spots
Lack of visibility into identity-related activities can lead to undetected threats. Implementing comprehensive monitoring tools is necessary to identify and address these shadow identities.

Multi-cloud environments

Transitioning to multi-cloud environments introduces additional identity security challenges.

Diverse identity mechanisms
Each cloud platform may have its own identity management system, making it difficult to establish a unified security approach across multiple clouds. This diversity can lead to inconsistencies and potential security gaps.

Integration difficulties
Ensuring seamless communication and secure access between resources across different cloud providers requires robust integration strategies, which can be complex to implement effectively.

Policy inconsistencies
Managing and enforcing consistent security policies across multiple cloud platforms is challenging due to varying features and capabilities, increasing the risk of security breaches.

What should be your approach to identity security?

Securing digital identities in a combination of multi-cloud and on-premise environments requires a balanced combination of proactive and reactive strategies. Proactive measures aim to prevent security incidents before they occur, while reactive measures focus on responding to and mitigating the impact of incidents that have already happened.

Proactive measures:

Implementing proactive security measures involves anticipating potential threats and establishing defenses to prevent breaches. Key proactive strategies include:

- **Implement strong access controls:** Establish robust access controls to ensure that only authorized individuals can access specific resources, reducing the risk of unauthorized data exposure.
- **Zero Trust architecture:** Adopt a Zero Trust model, which operates on the principle of "never trust, always verify," requiring continuous verification of user identities and device integrity, regardless of their location within or outside the network perimeter.
- **Privileged Access Management (PAM): I**mplement Privileged Access Management to monitor and control access to critical systems by users with elevated permissions, ensuring that administrative access is granted only when necessary and is properly monitored to prevent misuse.
- **Principle of Least Privilege (PoLP):** Apply the Principle of Least Privilege by granting users only the minimum level of access necessary to perform their job functions, limiting potential attack vectors and reducing the impact of accidental or malicious actions.

Reactive measures

Reactive security measures are essential for effectively responding to and mitigating the impact of security incidents. Key reactive strategies include

- **Incident response planning:** Establishing a clear incident response plan enables organizations to act swiftly when a security breach occurs. This includes defining roles and responsibilities, communication protocols, and steps for containment and recovery.

- **Continuous monitoring and threat detection:** Implementing tools like ITDR (Identity Threat Detection and Response) provide real-time monitoring of user activities and access patterns helps detect anomalies that may indicate a security breach. Early detection allows for prompt response to minimize potential damage.

- **Post-incident analysis and remediation:** After a security incident, conducting a thorough analysis to understand the root cause is crucial. This enables organizations to implement corrective actions and improve security measures to prevent similar incidents in the future.

By integrating both proactive and reactive approaches, organizations can establish a comprehensive identity security strategy that not only prevents potential threats but also effectively addresses incidents when they occur, ensuring robust protection of digital identities across cloud environments.

To summarise, the BFSI sector faces risks ranging from compromised credentials from phishing or brute-force attacks, overprivileged access accumulation by users or AI agents, and misconfigured access controls: each increasing the likelihood and impact of breaches, as seen in high-profile incidents. Weak or unsecured APIs expose systems to unauthorized actions, while token theft and prompt injection pose emerging threats through AI agents.

Together, these vulnerabilities create a high-stakes landscape where identity security must be both comprehensive and adaptive. Here is where you need a trusted identity security partner.

Securing the identity perimeter

Securing identities within cloud environments in the Banking, Financial Services, and Insurance (BFSI) sector presents a unique set of risks. Financial institutions are prime targets for cyber threats, including account takeovers, privilege escalation, and data breaches, which can have severe financial and reputational consequences.

To address critical risks and ensure comprehensive protection, we need deep visibility into identity activities and to detect suspicious behaviour, such as unauthorized access or unusual privilege escalation, at the earliest stage. Continuous monitoring and rapid response capability are needed for institutions to minimize the impact of potential breaches, ensuring that threats are neutralized before they can compromise critical

systems. Automated workflows and policy enforcement mechanisms are crucial in reducing the risk of human error, ensuring consistent, real-time adjustment of access controls, and providing rapid mitigation in case of an incident.

Unosecur's integrated approach is specifically designed to address the most pressing identity-related security risks, such as fraud, unauthorized access, and insider threats. By maintaining strict control over who can access what data, under which conditions, and for how long, financial institutions can significantly reduce their exposure to these threats.

Moreover, this approach supports compliance with stringent regulations, such as PCI-DSS, SOC2, and ISO 27017, while helping to preserve customer trust and financial integrity. Through this proactive identity security posture, BFSI organizations can operate with confidence, knowing that their critical systems and data are protected from evolving cyber threats.

Unosecur provides a comprehensive suite of tools designed to mitigate these risks. By combining proactive measures, such as real-time monitoring and advanced analytics, with reactive capabilities like automated incident response, Unosecur ensures that organizations are prepared to prevent and swiftly address potential identity-related security incidents, ultimately safeguarding sensitive financial data.

Here is how our tailored solutions, designed to enhance identity security and streamline compliance for BFSI organizations, give you a distinctive improvement in your security posture.

ISPM / Identity Fabric

Identity Security Posture Management (ISPM) is a strategic approach to continuously assess, monitor, and improve the security posture of an organization's identity systems. It focuses on identifying vulnerabilities, managing access risks, ensuring compliance, and enabling rapid incident response.

Identity Fabric, a key component or enabler of our ISPM, is a flexible, integrated framework for managing digital identities across diverse platforms and systems. It provides a graphical representation of the identity lifecycle, mapping out the integrated framework or architecture for managing identities across multiple systems (on-prem, cloud, SaaS) in a scalable and unified way, orchestrating and unifying identity policies, entitlements, and access management.

It provides a unified, scalable approach to securing both human and machine identities, supporting key functions like Single Sign-On (SSO), Multi-Factor Authentication (MFA),

Privileged Access Management (PAM), and identity governance. This interconnected structure enables organizations to adapt to changing technologies, third-party integrations, and evolving security threats, all while maintaining control and visibility over their identity data. Our cloud identity management service includes ISPM, which continuously assesses and strengthens your identity systems through real-time monitoring, risk assessments, and compliance management. With Identity Fabric, we provide a flexible, integrated framework that secures both human and machine identities.

ITDR

At Unosecur, we have perfected ITDR as a key component of our cloud identity management services. ITDR provides proactive, real-time monitoring of identity activities, using advanced analytics and machine learning to detect suspicious behavior such as unauthorized access or privilege escalation.

Our solution automatically responds to potential threats—locking compromised accounts, enforcing MFA, and triggering alerts – minimising risk before it impacts your organization.

The geofencing and time-boundaries capability lets users zero in on the most relevant issues while reducing false positives. Furthermore, the quarantine feature lets you block bad actors quickly, reducing MTTR to as low as 5 minutes.This ensures comprehensive protection against account takeovers, fraud, and data breaches while maintaining regulatory compliance. With ITDR, your organization can confidently manage access, reduce vulnerabilities, and safeguard sensitive data, all while staying ahead of evolving cyber threats.

NHI Dashboard

Managing non-human identities (NHIs), such as service accounts, API keys, and machine roles, is crucial for securing automated processes within BFSI organizations. These identities often have elevated privileges, which can lead to significant security breaches if compromised. With Unosecur's NHI Dashboard, we make it easier to monitor and manage NHIs by showing how they are used in real-time, which helps identify any misuse or excessive access. The level of visibility and control we offer enhances the security of automated financial systems, APIs, and services, providing your organization with greater confidence in its day-to-day operations.

Privileged Access Management (PAM) for cloud

As part of our comprehensive cloud identity management services, we provide

Privileged Access Management (PAM) for the cloud to secure and oversee access to your critical cloud resources. Our PAM solution ensures that privileged accounts — such as admin accounts, API keys, and machine roles — are effectively managed and monitored to prevent unauthorized access.

When a developer or user requires elevated privileges, they must submit a request through a formal process. This request undergoes a "four-eye" review, where approval is required from designated approvers via channels like Slack or other communication tools. This process ensures that only authorized users can gain access to sensitive resources.

In addition to this, our solution offers robust monitoring. Unosecur actively tracks privileged user activity, storing logs for all access events and providing real-time risk detection to flag any suspicious behavior. This enhanced monitoring helps identify potential threats before they can impact your cloud environment.

Features like Just-in-Time (JIT) access enforce the principle of least privilege to reduce the attack surface and mitigate the risk of privilege escalation or misuse. Our PAM solution also ensures compliance with industry regulations by maintaining detailed audit logs and providing continuous visibility over privileged access.

By integrating PAM for Cloud, you can manage access to sensitive data and applications securely, confident in the protection and integrity of your cloud infrastructure.

Identity compliance for BFSI organizations

For organizations in the BFSI sector, maintaining compliance with industry-specific regulations like PCI DSS, SOC2, and ISO27001 is essential for safeguarding sensitive financial data and preserving customer trust. Unosecur simplifies this process by offering proactive identity compliance checks, ensuring financial institutions stay aligned with regulatory standards. The platform identifies failing controls and provides actionable remediation steps, allowing BFSI organizations to take immediate corrective action.

Our compliance dashboard offers continuous monitoring of compliance status, reducing the risk of non-compliance during audits. By automating control tracking and providing real-time alerts, Unosecur eliminates the risk of human error and ensures that compliance requirements are consistently met. This enables financial institutions to avoid penalties, maintain regulatory adherence, and focus on their core business functions with confidence.

IAM Ops and IAM Analyzer

IAM (Identity and Access Management) is crucial for controlling user access to sensitive financial data and systems, ensuring that only authorized individuals can access critical resources. In the BFSI sector, IAM helps mitigate security risks, maintain compliance with regulations, and prevent internal and external threats by managing permissions and monitoring user actions in real time.

As BFSI sector businesses deal with highly sensitive financial data, there are strict regulatory requirements around data protection and access control. Protecting sensitive financial data is critical for their successful operation, and Unosecur's IAM Ops module and IAM Analyzer help implement the principle of least privilege PoLP ruthlessly, in real-time continuously.

Unosecur's IAM Ops module is designed to manage this by providing fine-grained control over user entitlements. Through features like Just Enough Privileges (JEP) and Just-in-Time (JIT) access, BFSI organizations can minimize the risk of unauthorized access to critical systems, ensuring users only have the permissions necessary for a limited duration. This proactive approach to access management is particularly vital in environments with stringent regulatory requirements such as PCI DSS and ISO. The No-Code Policy Editor simplifies the creation of tailored IAM policies without requiring coding expertise, enabling quick responses to evolving security needs. IAM Ops' audit trail provides a comprehensive log of permission changes, ensuring transparency and accountability, which are essential for regulatory compliance in the BFSI sector.

Unosecur's IAM Analyzer plays a crucial role in identifying and mitigating security risks within the BFSI sector's complex and heavily regulated systems. What sets IAM Analyzer apart is its ability to provide granular control like never before. It allows security teams to define exactly who has access to which services and resources, and for what time period. This precision makes it easier to enforce the principle of least privilege and ensures that permissions are always aligned with business needs and security policies. Leveraging both of these enhances the organization's security posture, reduces exposure to internal and external threats, and ensures compliance with industry regulations — all while safeguarding customer trust and financial integrity.